Kriptovalute – novac budućnosti

Tomislav Kućar
Algebra/Primjenjeno računarstvo, Zagreb, Hrvatska
kucar.tomislav@gmail.com

***Sažetak* – Iako su osnovni koncepti postavljeni već 90ih kriptovalute dobivaju na popularnosti tek posljednih nekoliko godina. U svojem radu analiziram važnost i način rada kriptovaluta te dodatno analiziram najpopularniju valutu bitcoin.**

Ključne riječi – kriptovalute; blockchain; bitcoin; digitalni potpis; rudaranje

I. KRIPTOVALUTE

Potrebu za kriptovalutama 1994 izlaže Timothy May, njegova ideja je stvoriti društvo u kojem su tajnost i privatnost glavna načela a koje bi se baziralo na anonimnim novčanim transakcijama [1].

May-eva ideja postaje široko prihvaćena od strane mnogih aktivista i istraživača, koji su počeli ulagati vrijeme i resurse u stvaranje praktične primjene kriptografije. Wei Dai 1998 stvara osnovnu specifikaciju protokola za takozvani B-money koji je bio praktične prirode i predstavljen kao rezultat May-eve Kripto-anarhije [2]. B-money je postao temeljem modernih kriptovaluta i osnova na kojoj je 10 godina kasnije izgrađen bitcoin, prva decentralizirana, javno dostupna kriptovaluta.

Kriptovalute postaju sve više zastupljene i time postavljaju izazov za fiat valute. Kod kriptovaluta ne postoji centralna organizacija koja kontrolira nastajanje novca te nisu podložne niti jednom državnom regulatornom tijelu. Kod fiat valuta države ili nacionalne banke ispisuju novac, u slučaju kriptovaluta novi novac nastaje procesom "rudarenja". Rudarenje u smislu kripto valuta označava kompleksno heširanje i metodologije vremenskih oznaka kako bi se označila svaka "kovanica" unutar valute [3]. Sustavi kriptovaluta pružaju anonimne decentralizirane transakcije. Ova anonimnost štiti korisnikov identitet i privatnost. To dovodi do velike inicijalne prihvaćenosti na crnim tržištima.

Prihvaćenost i broj korisnika se svake godine povećava u stotinama puta. Trenutno postoje desetci izrazito snažnih valuta i stotine manjih, nadalje diljem svijeta u gotovo svakoj zemlji postoji veliki broj online ali i fizičkih mjenjačnica u kojima se kriptovalute mogu mjenjati za fiat. Internacionalne tvrtke su već uvele bitcoin a i neke druge veće kriptovalute kao jedan od načina plaćanja, neke od poznatijih su Wikipedia, Microsoft i Steam [4]. Čak i u hrvatskoj se sa bitcoinom može platiti šišanje u zagrebu, kavu ili čak bravarske usluge. Također postoji nekoliko bankomata na kojima se bitcoin može kupiti ili prodati za fiat novac (kunu).

II. BITCOIN

Bitcoin je prva decentralizirana kriptovaluta, pokrenuta u 2008 na temelju rada pseudoanonimnog istraživača i razvijatelja Satoshi Nakomota. Bitcoin nije organizacija ili tvrtka već standard i protokol. Funkcionira na jednostavnim matematičkim pravilima i svatko tko sudjeluje na mreži suglasan je sa pravilima na koji način protokol i mreža funkcioniraju. U prosincu ove godine bitcoin doseže cjenu od 19891,00 $ po kovanici [5].

A. Transakcije i blockchain

Bitcoin transakcije se propagiraju na peer to peer mreži nakon nastanka, validiraju se i konačno dodaju na globalni zapis svih transkacija (blockchain). Transakcije su šifrirani strukturni podatci koji služe za prijenos vrijednosti između dva sudionika na mreži. Pošto je svaka transakcija javni unos u blockchainu, on se može promatrati kao novi oblik knjigovodstvene knjige sa trostrukim unosom.

Životni ciklus transakcije započinje sa kreacijom iste. Transkacija je potpisana sa digitalnim potpisima koji ukazuju da je transkacija autorizirana. Nakon autorizacije sljedi emitiranje iste na bitcoin mrežu gdje svako mrežno čvorište (sudionik) validira i propagira transakciju sve dok ne stigne do gotovo svih čvorišta na mreži. Konačno transakcija je verificirana od jednog rudara (mining node) i uključena u jednan blok transakcija koji je zapisan na blockchain.

Jednom zapisana na blockchain i potvrđena od dovoljno daljnjih blockova (potvrda), transkacija je permanentan dio bitcoin knjige svih zapisa (ledger/blockchain) prihvaćena je i validirana od strane svih sudionika. Bitcoin dodijeljen novom “vlasniku” može sada biti potrošen u novoj transakciji.

B. Arhihektura

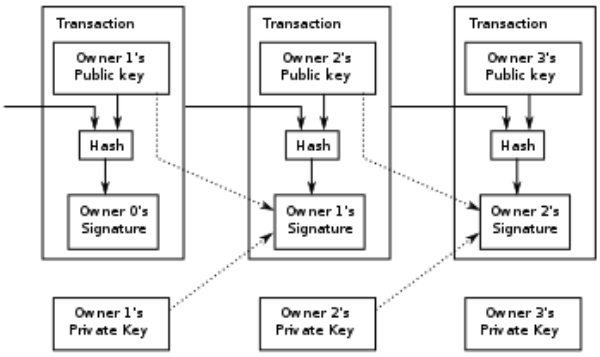
Kako bi razumjeli način rada i arhihekturu bitcoina potrebno je objasniti osnovne pojmove i poznavati osnove kriptografije. Kovanica je lanac digitalno potpisanih certifikata. Transakcija je proces u kojem kovanica digitalno potpisuje heš prošle transakcije javnim ključem primatelja i dodaje ga na kraj kovanice. Server vremenskih otisaka sadrži vremenske otiske svake dosadašnje transakcije. Blok je kolekcija transakcija koje se trebaju potvrditi i broadcastati pomoću grana koje vrte bitcoinov središnji motor.

Svaki blok je Merkle Root transakcije što znači da svaki blok sadrži heš prijašnjeg bloka i izraz kako bi se zadovoljili zahtjevi hešing funkcije koja je u slučaju bitcoina SHA-256. Jednom ostvarena transakcija se broadcasta svim granama u mreži. Grane stvaraju blok transakcija i rade na pronalasku rješenja za svoj blok. Rješenje je potvrdni korak u kojem grane koriste računalne resurse sa ciljem pronalaska izraza koji je potrebanza ostvarenje zahtjeva hešing algoritma. Jednom izračunato rješenje se broadcasta svim granama u mreži a blok se dodaje u blockchain.

C. Rudarenje

Rudarenje je usluga održavanja zapisa pomoću računalnih resursa. Rudari drže blockchain konzistentnim, kompletnim i nepromjenjivim konstantnim provjerama i prikupljanjem novih transakcija. Svakih 2016 blokova odnostno 14 dana (pod pretpostavkom da novi blok nastaje svakih 10min) težina algoritma se povećava sa ciljem održavanja 10 minutnog intervala između blokova. Na taj način sustav se automatski prilagođava ukupnoj količini računalnih resursa na mreži [6].

Između 1. ožujka 2014. i 1. ožujka 2015. prosjećni broj izraza koje su rudari morali proći prije stavranja novog bloka povećao se sa 16.4 na $200.5*10^{18}$ [7].



Sl1. Pojednostavljeni lanac vlasništva

Sustav digitalnog potpisivanja i lanac blokova čine modifikacije blockchaina gotovo nemogućima pošto bi napadač trebao modificirati sve trenutne blokove kako bi njegov bio prihvaćen. Kako se novi blokovi kontinuirano stvaraju svakim trenutkom kompleksnost napada postaje veća.

D. Slabe točke

Nedostatak bitcoina je što jednom pokrenut protokol i sustav se ne mogu znatno uređivati i mjenjati. To znači da svaka slabost i slaba točka koje se mogu otkriti u budućosti mogu ugroziti egzistenciju cjelog sustava. Do sada su već otkrivene i iskorištavane određene slabosti, ovdje navodim dvije poznatije.

1) 51 postotni napad: trenutno je ovo najveća opasnost za postojanje bitcoina, napad podrazumjeva situaciju u kojoj 51 posto rudara ulazi u zajednicki računalni bazen i na taj način može donositi odluke za svaki novi blok. To omogućaca bazenu da troši novac koji mu ne pripada (dvostruko trošenje). Bitcoin protokol je dizajniran u vjeri da će u svakom trenutku 51% rudara biti pošteno. No unatoč tome sustav nasumično odabire rudare razbijajući time bazene računalnih resursa i time sprječava napade ove vrste.

2) Problem dvostrukog trošenja: svaka transakcija prosječno treba čekati 10min da ju sustav potvrdi. To vrijeme čekanja nije prihvatljivo za sustave i korisnike koji trebaju instantno procesiranje transakcija. Ova situacija dovodi do problema dvostrukog trošenja bez 51 postotnog napada. Istraživači su uspješno izvršili ovaj napad broadcastom lažne transakcije velikom broju grana uz ispravne transakcije. Ovo rezultira u potvrdi od strane mreže pošto većina grana potvrđuje pozitivne transakcije [8].

III. ZAKLJUČAK

Iako postoje već više od 20 godina kripto valute su tek u ranim povojima. Iako vlade diljem svijeta pružaju otpor vidimo da valute poput bitcoina pronalaze svoju primjenu u svakodnevnom životu. Bitcoin je novi oblik gotovine i sigurno je zaključiti kako su kriptovalute novac budućnosti.

LITERATURA

[1] Timothy C. May, The Cyphernomicon, 09.10.1994

[2] Wei Dai, B-money, http://www.weidai.com/bmoney.txt

[3] https://en.wikipedia.org/wiki/Bitcoin#Mining

[4] Jonas Chokun. Who accepts bitcoins as payment? list of companies, stores, shops. https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins, 2017

[5] https://cryptowat.ch/bitfinex/btcusd/3d

[6] Andreas M. Antonopoulos, *Mastering Bitcoin. Unlocking Digital Crypto-Currencies.* O'Reilly Media, 2014

[7] "Difficulty History" (The ratio of all hashes over valid hashes is D x 4,295,032,833, where D is the published "Difficulty" figure.). Blockchain.info

[8] Danny Bradbury. The problem with bitcoin. Computer Fraud & Security, 2013.